ดร.วิรินทร์ แผนประดิษฐสิน

บริหารจัดการเครือข่ายแบบหลายระบบปฏิบัติการสำหรับ SMEs

การบริหารการจัดการเครือข่าย เพื่อเพิ่มประสิทธิภาพให้สูงขึ้น และทำงานได้เร็วขึ้น เพื่อให้เหมาะสมกับธุรกิจขนาดกลางและขนาดย่อม

ปัจจุบันการใช้งานคอมพิวเตอร์ในรูปแบบของเครือข่ายภายในองค์กรมีมากขึ้นเรื่อย ๆ การพัฒนาเทคโนโลยีของเครือข่าย รวมทั้งระบบปฏิบัติการเครือข่ายได้รับการพัฒนาให้ประสิทธิภาพสูงขึ้นเรื่อย ๆ ทำงานเร็วขึ้น ให้ความร่วมมือในการทำงานกับระบบปฏิบัติการอื่น ๆ ได้ดีขึ้น ใช้ทรัพยากรคอมพิวเตอร์ เช่น หน่วยความจำ และเนื้อที่ของดิสก์มากขึ้น รวมทั้งสามารถสนับสนุนการทำงานของโปรโตคอลในรูปแบบต่าง ๆ ได้มากกว่าและดีกว่าแต่ก่อน อย่างไรก็ดีนับตั้งแต่เริ่มมีการนำระบบเครือข่ายคอมพิวเตอร์ไปใช้ในองค์กรเรื่อยมาจนปัจจุบัน ทำให้ท่านได้รู้จักกับระบบปฏิบัติการต่าง ๆ กว่า 5 ระบบ เป็นที่เรียบร้อยแล้ว ซึ่งได้แก่ OS/2, Novell NetWare 2.x-5.1, Windows NT, Windows 2000 Server และระบบปฏิบัติการ UNIX รวมทั้ง LINUX เป็นต้น

ระบบปฏิบัติการเหล่านี้มีจุดแข็งในการทำงานที่ไม่เหมือนกัน แต่ละระบบอาจเหมาะกับแอพพลิเคชันบางชนิด เช่น งานที่เกี่ยวกับระบบไฟล์จะเหมาะสำหรับ NetWare ส่วนแอพพลิเคชันรวมทั้งฐานข้อมูลเหมาะสำหรับ Windows NT และ UNIX เป็นต้น

องค์กรขนาดเล็กและขนาดกลางโดยทั่วไปมักจะใช้ระบบปฏิบัติการสำหรับเครือข่ายมากกว่าหนึ่งแบบเสมอ ซึ่งผลที่ติดตามมาคือการบริหารจัดการเพื่อให้การทำงานเป็นหนึ่งเดียว (โดยผู้ดูแลคนเดียวกัน) เป็นเรื่องยาก

แนวทางบริหารจัดการเครือข่ายที่ใช้หลายระบบปฏิบัติการ

ระบบเครือข่ายตามองค์กรธุรกิจระดับย่อมและระดับกลางจำนวนไม่น้อยที่ใช้ระบบปฏิบัติการหลายตัวบนเครือข่ายขององค์กรเดียวกัน สาเหตุที่เป็นเช่นนี้สามารถแยกออกได้ 2 สาเหตุ ได้แก่ การเลือกระบบปฏิบัติการที่ต่างจากที่มีอยู่แล้ว เพราะถูกบังคับโดยแอพพลิเคชันที่ใช้ เช่น โปรแกรมสำเร็จรูปบางตัวออกแบบมาให้ทำงานบนระบบปฏิบัติการจำเพาะเจาะจง เช่น ระบบปฏิบัติการ UNIX เป็นต้น ประการต่อมาเกิดจากความรู้สึกตามกระแสว่าแอพพลิเคชันที่จะใช้ต้องทำงานบนโหมดกราฟิกเท่านั้นจึงจะทันสมัย ทั้งที่งานบางประเภทหากไม่ใช้กราฟิกยังสามารถทำงานได้รวดเร็วกว่า เช่น การโอนย้ายถ่ายแฟ้มข้อมูลสำหรับแอพพลิเคชันบางตัวที่ทำงานบนโหมด DOS เป็นต้น นอกจากนี้ยังมีปัญหาจากความไม่เข้าใจระบบปฏิบัติการของเครือข่าย รวมทั้งได้รับการติดตั้งระบบปฏิบัติการของเครือข่ายมาพร้อมกับเครื่องคอมพิวเตอร์ที่จัดซื้อมา

ไม่ว่าเครือข่ายของท่านจะใช้ระบบปฏิบัติการกี่ตัว สิ่งที่ปฏิเสธไม่ได้คือปัญหาของการจัดการที่จะเกิดขึ้นอย่างแน่นอน รวมทั้งปัญหาหลักที่ต้องตามมา ได้แก่ การทำงานร่วมกันของระบบปฏิบัติการที่แตกต่างกัน

ปัญหาเหล่านี้สามารถแก้ไขได้ หากจะแยกประเด็นปัญหาออกเป็น 2 ส่วน ได้แก่ ส่วนที่หนึ่งคือส่วนของระบบปฏิบัติการเครือข่ายเฉพาะรายการ ส่วนที่สองได้แก่ส่วนของปัญหาที่เกิดขึ้นจากการทำงานร่วมกันของระบบปฏิบัติการที่ต่างกันบนเครือข่ายเดียวกันเหล่านี้

แม้ว่าองค์กรบางแห่งใช้วิธีแยกเครือข่ายที่มีระบบปฏิบัติการต่างกันออกจากกัน ก็ตาม ซึ่งการกระทำเช่นนี้ดูจะไม่สอดคล้องกับคำว่าระบบเครือข่ายที่แท้จริง เนื่องจากระบบเครือข่ายที่สมบูรณ์ต้องมีการเชื่อมโยงถึงกันหมด เพื่อให้ทรัพยากรบนเครือข่ายได้รับการแบ่งปันกันตามความเหมาะสม โดยถ้วนหน้าแม้จะมีระบบปฏิบัติการต่างกัน

ปัญหาที่เกิดจากระบบปฏิบัติการเครือข่ายเฉพาะ

ปัญหาที่อาจเกิดขึ้นกับระบบปฏิบัติการแบบเฉพาะเจาะจงนี้มักได้แก่ปัญหาติดขัดของไฟล์เซิร์ฟเวอร์ อันมีสาเหตุมาจากการจัดตั้งค่าคอนฟิกของระบบปฏิบัติการไม่ถูกต้องหรือพอเพียง นับตั้งแต่การเลือกใช้อุปกรณ์ฮาร์ดแวร์ที่ไม่สอดคล้องกับความต้องการของระบบปฏิบัติการ จนถึงปัญหาของการบริหารจัดการ

ปัญหาที่เกิดจากการดูแลหลายระบบปฏิบัติการ

ปัญหาส่วนนี้สามารถแบ่งออกเป็นหัวข้อได้ดังนี้

- ความเข้ากันได้ของระบบปฏิบัติการแบบต่าง ๆ
- การโอนย้ายถ่ายไฟล์ระหว่างกัน
- ปัญหาการแบ่งปันใช้งานทรัพยากรบนเครือข่ายร่วมกัน
- การสื่อสารระหว่างระบบปฏิบัติการแบบต่าง ๆ

อย่างไรก็ดีปัญหาต่าง ๆ เหล่านี้สามารถแก้ไขได้หากมีการบริหารจัดการที่ดีและเป็นไปตามหลักวิชาการ

งานของผู้ดูแลเครือข่าย

งานหลักของผู้ดูแลหรือจัดการเครือข่าย ไม่ว่าการดูแลจัดการเครือข่ายภายใต้ระบบปฏิบัติการที่เหมือนกันหรือต่างกัน สามารถแยกเป็นหัวข้อหลักดังนี้

- การจัดการให้เกิดการทำงานร่วมกันของระบบปฏิบัติการต่าง ๆ (Interoperability)
- การบริหารจัดการกับเซิร์ฟเวอร์ของเครือข่าย (Server Management)
- การบริหารจัดการกับระบบรักษาความปลอดภัย (Security Management)
- การบริหารจัดการกับเครื่องพิมพ์หรือทรัพยากรอื่นบนเครือข่าย (Network Resource Management)
- การบริหารจัดการเพื่อการกู้คืนและสำรองข้อมูล (Data Recovery & Backup)
- การเฝ้าดูและปรับแต่งประสิทธิภาพของเซิร์ฟเวอร์ (Server Monitoring & Optimization)
- การบริหารจัดการแอพพลิเคชันบนเครือข่าย (Application Management)
- การวิเคราะห์จุดเสียและการแก้ไขปัญหา (Troubleshooting)

การจัดการให้เกิดการทำงานร่วมกันของระบบปฏิบัติการต่าง ๆ

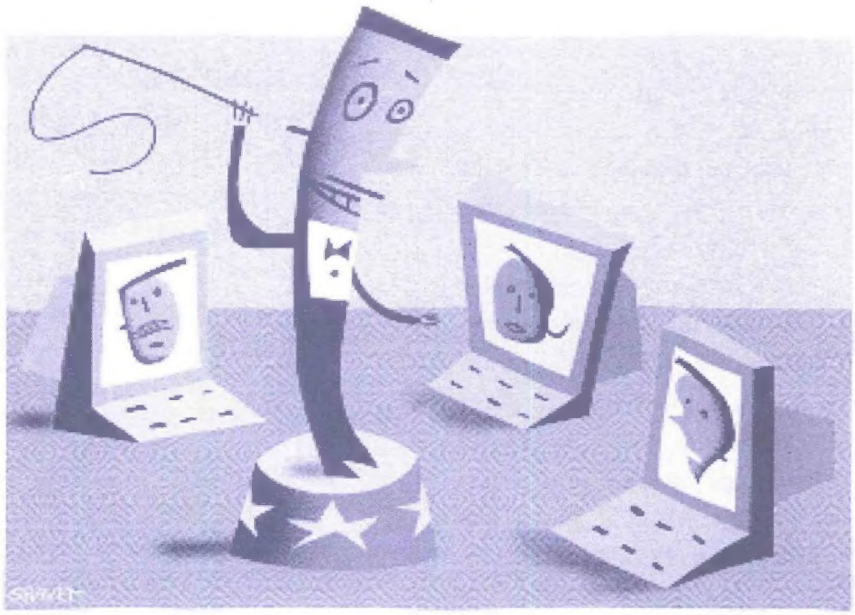
ปัญหาที่ว่าทำไมการทำงานร่วมกันของระบบปฏิบัติการต่าง ๆ จึงมีความสำคัญ

เป็นที่ทราบดีว่าเครือข่ายในองค์กรขนาดกลางทั่วไปมักจะประกอบด้วยระบบปฏิบัติการที่แตกต่างกันมาผสมกันที่เรียกว่า Heterogeneous Networking จากข้อมูลพบว่า เครือข่ายองค์กรในบ้านเราประกอบด้วยระบบปฏิบัติการ Windows NT และ NetWare เป็นหลัก รวมทั้งระบบปฏิบัติการ UNIX จำนวนหนึ่ง ซึ่งระบบปฏิบัติการต่าง ๆ เหล่านี้สามารถทำงานเข้าขากันได้ และกุญแจสำคัญของการทำงานร่วมกันนั้นประกอบด้วยส่วนสำคัญ 4 ประการ ได้แก่

1. การบริหารจัดการ (Management) ในที่นี้ครอบคลุมถึงการจัดการเกี่ยวกับระบบรักษาความปลอดภัย การบริหารจัดการไดเรคทอรี และการบริหารจัดการเกี่ยวกับระบบ (System Management)

2. ส่วนที่เป็นแอพพลิเคชันที่ครอบคลุม Presentation หรือ Transaction และส่วนที่เป็นคอมโปเนนต์ (ส่วนประกอบการทำงานในแอพพลิเคชันนั้น ๆ)

3. ข้อมูล (Data) ในที่นี้จะครอบคลุมถึงการเข้าถึงเพื่อใช้แฟ้มข้อมูลหรือการเข้าถึงเพื่อใช้งานฐานข้อมูล การทำ Replication รวมทั้งการเข้าถึงเพื่อใช้อีเมล์และการจัดเก็บ



4. เครือข่าย (Network) ในที่นี้ได้แก่ โปรโตคอลและการบริการงานพิมพ์ เป็นต้น

นั่นหมายความว่าระบบปฏิบัติการแต่ละแบบต้องเอื้ออำนวยให้ส่วนประกอบที่กล่าวมาแล้วทั้ง 4 ประการสามารถทำงานร่วมกันภายใต้ระบบที่ต่างกัน เช่น สามารถโอนย้ายข้อมูลข่าวสารไปมาระหว่างกัน สามารถใช้ทรัพยากรเครือข่ายเดียวกันภายใต้ระบบที่ต่างกันได้ รวมทั้งจะต้องสามารถสื่อสารกันได้ การกระทำเช่นนี้จะก่อให้เกิดประโยชน์หลายประการดังนี้

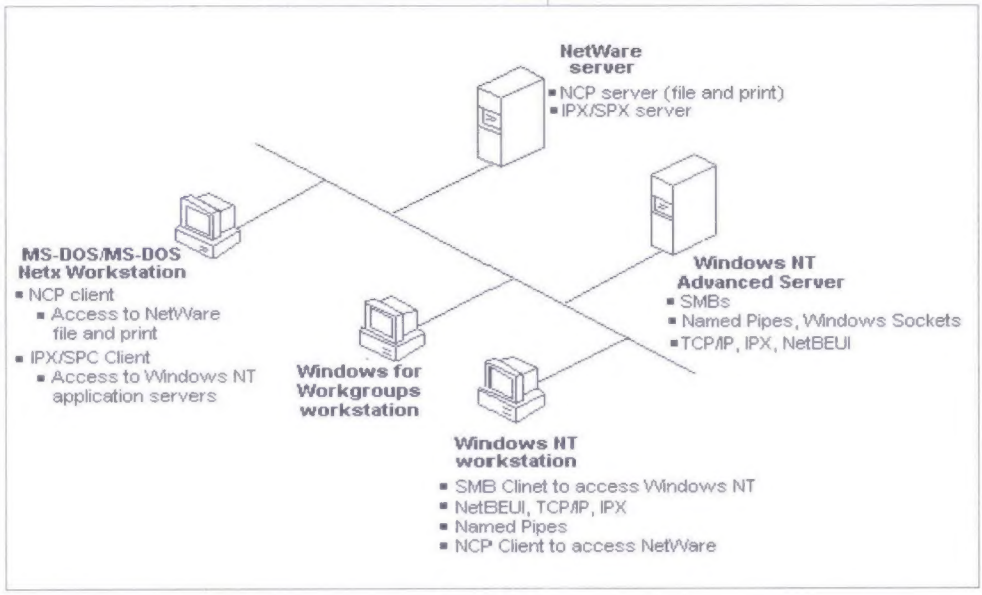
1. ช่วยลดค่าใช้จ่ายในการดำเนินงานและความซับซ้อน การที่ระบบปฏิบัติการต่าง ๆ สามารถทำงานร่วมกัน จะช่วยให้ลดต้นทุนในการดำเนินงาน เพื่อรองรับการทำงานของระบบที่ต่างกันเหล่านี้ได้

2. ช่วยประหยัดค่าใช้จ่ายในการติดตั้งจัดซื้ออุปกรณ์บนเครือข่าย เพื่อรองรับการทำงานบนระบบปฏิบัติการที่แตกต่างกัน เป็นที่น่ายินดีว่าระบบปฏิบัติการเครือข่ายตัวหลัก ๆ เช่น Windows NT หรือ Windows 2000 Server รวมทั้งระบบปฏิบัติการอื่น ๆ เช่น NetWare และระบบปฏิบัติการ UNIX ล้วนแต่สามารถทำงานร่วมกันบนเครือข่ายเดียวกันได้ทั้งสิ้น ที่ทำเช่นนี้ได้เป็นผลมาจากประสิทธิภาพการทำงานของระบบปฏิบัติการเองที่มีกลไกเชื่อมโยงการทำงานระหว่างระบบปฏิบัติการที่ต่างกัน นอกจากนี้บางระบบปฏิบัติการยังต้องพึ่งพาซอฟต์แวร์จากผู้ผลิตรายอื่น เพื่อให้ระบบปฏิบัติการที่ต่างกันสามารถทำงานร่วมกันได้ ซึ่งมีชื่อเรียกว่า Middleware

ผู้เขียนจะอธิบายถึงความเข้ากันได้ของระบบปฏิบัติการ Windows NT ในมุมมองต่าง ๆ ดังนี้

- **การทำงานร่วมกับ NetWare Server**

หากท่านวางระบบเครือข่าย Windows NT อยู่แล้ว แต่ต้องการสื่อสารกับเครือข่ายที่ใช้ NetWare เรื่องนี้ไม่ต้องเป็นกังวล เนื่องจาก Windows NT ของไมโครซอฟท์มีเครื่องมือที่ใช้สื่อสารกับระบบปฏิบัติการ NetWare ที่ให้มาพร้อมเรียกว่า NWLINK ซึ่งเป็นโปรโตคอล IPX/SPX ขนาด 32 บิต



รูปที่ 1 แสดงการเชื่อมต่อแบบหลายระบบปฏิบัติการในหนึ่งองค์กร

สำหรับ NetWare รวมทั้งซอฟต์แวร์บริการที่ชื่อว่า Gateway Services for NetWare (GSNW) ซึ่งจะทำให้ผู้ใช้ (Client) ที่ทำงานบน Windows สามารถเข้าถึง NetWare Server ได้ นอกจากนี้ Windows NT ยังมีเครื่องมือที่ใช้โยกย้าย (Migration) สำหรับ NetWare เรียกว่า NWConv ซึ่งจะช่วยให้ผู้ดูแลเครือข่ายสามารถโยกย้ายผู้ใช้และแฟ้มข้อมูลจากเซิร์ฟเวอร์ที่ใช้ NetWare ไปสู่เซิร์ฟเวอร์ของ Windows NT

นอกจากนี้ไมโครซอฟท์ยังมีข้อเสนอเป็นทางเลือกที่จะทำให้การทำงานร่วมกันระหว่าง Windows NT กับ NetWare เป็นเรื่องง่ายยิ่งขึ้น รวมทั้งยังมีซอฟต์แวร์บริการสำหรับแฟ้มข้อมูลและงานพิมพ์สำหรับ NetWare ทำให้ผู้ใช้ที่ทำงานบน NetWare สามารถเข้าถึงแฟ้มข้อมูลและงานพิมพ์จาก Windows NT Server สุดท้ายได้แก่โปรแกรมบริการที่มีชื่อเรียกว่า Directory Service Manager for NetWare ซึ่งจะทำให้ผู้ดูแลเครือข่ายสามารถบริหารจัดการกับผู้ใช้บนเซิร์ฟเวอร์ของ NetWare หลายตัวได้โดยตรง รูปแบบการเชื่อมต่อเป็นไปดังรูปที่ 1

- **การทำงานร่วมกับ UNIX**

Windows NT กับ UNIX ต่างก็เป็นระบบปฏิบัติการเครือข่ายที่ถูกจัดให้เป็น Heterogeneous หรือมีความแตกต่างกันโดยลักษณะ การทำงานบางประการที่สำคัญ เช่น ระบบ UNIX มีความสามารถด้านมัลติยูสเซอร์ แต่ทั้งคู่มีสิ่งที่เหมือนกัน กล่าวคือ ต่างให้การสนับสนุนเครือข่ายหลายรูปแบบ รวมทั้งโปรโตคอลสำหรับการขนส่งข้อมูล (Transport Protocol) หลายแบบเช่นกัน นอกจากนี้ทั้งคู่ยังมีความคล้ายคลึงกันในเรื่องของระบบรักษาความปลอดภัย รวมทั้งขีดความสามารถที่จะเฝ้าตรวจสอบและติดตามการทำงานของผู้ใช้และระบบต่าง ๆ อีกด้วย

- **การทำงานร่วมกับ UNIX จาก NT**

File Manager และ Explorer ของ Windows NT ไม่สามารถเรียกดูแฟ้มข้อมูลที่ผ่านการจัดตั้งการแชร์เรียบร้อยแล้วของ UNIX หากไม่ได้ใช้โปรแกรมเสริมเข้าช่วย และมีทางเดียวที่จะโอนย้ายถ่ายแฟ้มข้อมูลโดยไม่ต้องใช้โปรแกรมเสริม ได้แก่ การใช้บริการ Internet Services

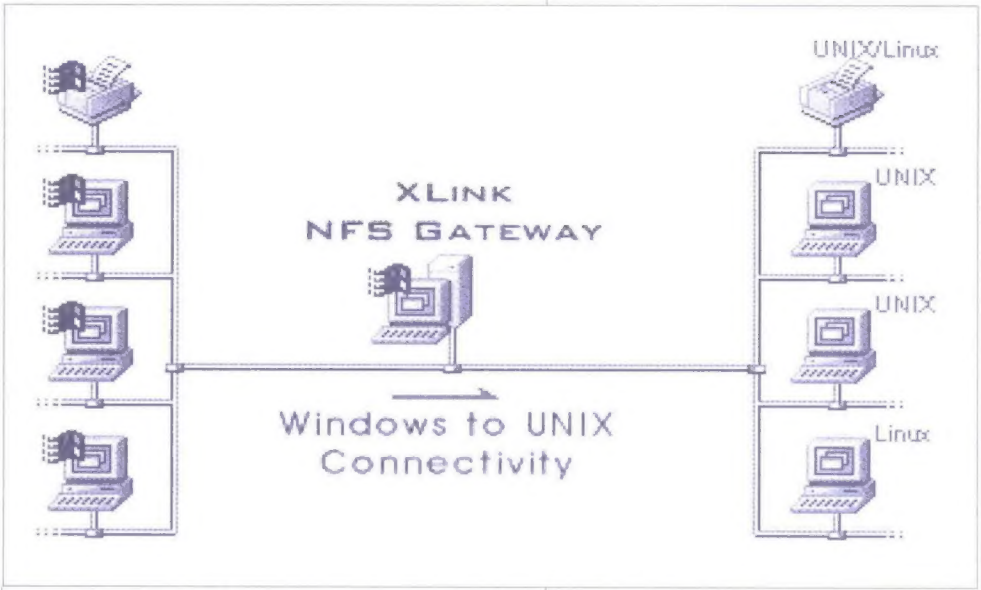
● **การทำงานร่วมกับ NT จาก UNIX**

จะต้องมีการติดตั้งระบบที่เรียกว่า Remote File System จาก Windows NT ไปไว้ที่ไฟล์ไดเรคทอรีของ UNIX ในกรณีที่ต้องการเข้าไปใช้งานโดยทางคำสั่ง UNIX (ดังรูปที่ 2)

นอกจากนี้ยังมีซอฟต์แวร์อีกตัวหนึ่งเรียกว่า Network File Sharing System หรือ NFS ซึ่งเป็นซอฟต์แวร์ดั้งเดิมบน UNIX ที่จะทำให้ผู้ใช้งานจาก Windows NT สามารถเข้ามาแบ่งใช้งานแฟ้มข้อมูลบนระบบ UNIX ในลักษณะที่เสมือนว่าผู้ใช้นั้นมาจากเครือข่ายภายในระบบ UNIX เอง การที่ Windows NT สามารถทำเช่นนี้ได้ต้องติดตั้งซอฟต์แวร์ที่ชื่อว่า NFS Gateway เสียก่อน ซึ่งซอฟต์แวร์นี้มาจากผู้ผลิตต่าง ๆ เช่น NFS Manaestro จาก Hummingbird หรือ Omni-NFS Gateway จาก HLink Technology โดยซอฟต์แวร์ทั้งหลายเหล่านี้จะทำหน้าที่เป็นเกตเวย์เมื่อติดตั้งลงบน Windows NT Server รวมทั้งซอฟต์แวร์ในส่วน Client แล้ว ผู้ใช้บน Windows NT จะสามารถเข้าไปแบ่งใช้งานแฟ้มข้อมูลของ UNIX ได้

อย่างไรก็ดีท่านยังสามารถใช้งานแอพพลิเคชันบางตัวที่มากับ Windows NT เช่น FTP และ Telnet ซึ่งเป็นแอพพลิเคชันที่สามารถทำให้ผู้ใช้งานจาก Windows NT สามารถเชื่อมต่อกับคอมพิวเตอร์ที่ทำงานบนระบบ UNIX เพื่อขอใช้งานแอพพลิเคชันและแบ่งปันข้อมูลบน UNIX อย่างไรก็ดีแอพพลิเคชันเหล่านี้ยังมีขีดจำกัด

สรุปในหัวข้อนี้คือการบริหารจัดการเกี่ยวกับเครือข่ายที่ใช้หลายระบบปฏิบัติการไม่ได้มีความซับซ้อนกว่าที่คิด เนื่องจากระบบปฏิบัติการหลักมักจะมีเครื่องมือเสริมที่เอื้ออำนวยความสะดวกในการที่ทำให้ระบบปฏิบัติการต่าง ๆ สามารถอยู่ร่วมกันได้บนเครือข่ายเดียวกัน ทำให้ประหยัดค่าใช้จ่ายในการดูแลและจัดการ รวมทั้งประหยัดทรัพยากรบนเครือข่ายได้อีกด้วย



รูปที่ 2 แสดงการใช้ Gateway เพื่อเชื่อมต่อระหว่าง Windows กับ UNIX

การบริหารจัดการกับเซิร์ฟเวอร์ของเครือข่าย

การบริหารจัดการกับเซิร์ฟเวอร์ที่ใช้ระบบปฏิบัติการหลากหลาย เช่น Windows NT/2000 Server, UNIX Server รวมทั้ง NetWare Server (ในที่นี้จะครอบคลุมทุกเซิร์ฟเวอร์ที่ทำงานบนระบบปฏิบัติการดังที่กล่าวมาแล้ว ซึ่งได้แก่ Application Server, Database Server, Web Server, Proxy Server, Groupware Server, Print Server และ FAX Server) มองแล้วอาจเป็นเรื่องยาก เนื่องจากในแต่ละระบบปฏิบัติการมีวิธีการบริหารจัดการที่ต่างกัน อย่างไรก็ดีสามารถแบ่งประเภทของงานที่จะต้องดูแลจัดการกับเซิร์ฟเวอร์ต่าง ๆ เหล่านี้เป็นงานย่อย ๆ ได้แก่

● การจัดการและติดตั้งค่า Configuration ของเซิร์ฟเวอร์ รวมทั้งปรับปรุงประสิทธิภาพในทางฮาร์ดแวร์ของเซิร์ฟเวอร์ เพื่อให้สอดคล้องกับความต้องการใช้งานในระบบปฏิบัติการและจำนวนผู้ใช้ รวมทั้งข้อมูลที่เปลี่ยนแปลง

● การดูแลการล็อกอินเข้ามาที่เซิร์ฟเวอร์ต่าง ๆ ของผู้ใช้งานจากเครื่องคอมพิวเตอร์บนเครือข่าย การเฝ้าดูการใช้ทรัพยากร เช่น แฟ้มข้อมูล หรือเครื่องพิมพ์ เป็นต้น การส่งข่าวสารเป็นการแจ้งเตือนไปยังผู้ใช้ การปรับปรุงแก้ไขบัญชีรายชื่อของผู้ใช้ การเพิ่มหรือลดทอนสิทธิ์ในการใช้งานบนเซิร์ฟเวอร์ และอื่น ๆ ที่ทำได้บนเซิร์ฟเวอร์

● การติดตั้งการจัดค่าหรือการปรับแต่งค่า Configuration ที่จำเป็น หรือการถอดถอนแอพพลิเคชันออกไปจากเซิร์ฟเวอร์ รวมทั้งการอัพเกรดตัวแอพพลิเคชันที่มีอยู่แล้วให้มีประสิทธิภาพสูงขึ้น ซึ่งการทำเช่นนี้อาจต้องแก้ไขเปลี่ยนแปลงส่วนประกอบที่สำคัญบางประการของระบบปฏิบัติการนั้น ๆ เช่น Registry ใน Windows NT หรือ 2000 Server เป็นต้น

● การติดตั้งและการจัดค่า Configuration ให้กับบริการบางตัวเพื่อผลแห่งประสิทธิภาพการใช้งานของเซิร์ฟเวอร์ เช่น การติดตั้งเซิร์ฟเวอร์ให้ทำหน้าที่เป็น FAX Server หรือ Local Server Based Router เป็นต้น ท่านอาจจะเลือกการติดตั้งและการตั้งค่า Configuration ให้โปรโตคอลของเครือข่ายเพื่อให้เซิร์ฟเวอร์นั้นสามารถตอบสนองความต้องการของท่านอย่างเต็มที่

● การติดตั้ง Client ไม่ว่าจะเป็น Client for DOS หรือ Windows 95/98 เพื่อเป็นลูกข่ายของเซิร์ฟเวอร์ Windows NT/2000 หรือ NetWare และ UNIX ก็ตาม

ระบบปฏิบัติการต่าง ๆ สามารถรองรับการจัดการบริหารเซิร์ฟเวอร์ด้วยเครื่องมือที่ให้มาพร้อม เช่น ในระบบ Windows NT จะมีเครื่องมือที่เรียกว่า Server Manager ส่วนในระบบ Windows 2000 จะมี MMC ซึ่งสามารถเรียกจากเมนู Start แต่ถ้าจะใช้ซอฟต์แวร์เสริม ท่านอาจเลือกใช้ Network ServaNT สำหรับ NetWare 4 และ 5 จะมีเครื่องมือที่ชื่อว่า ServerTrak ซึ่งเป็นซอฟต์แวร์เสริม

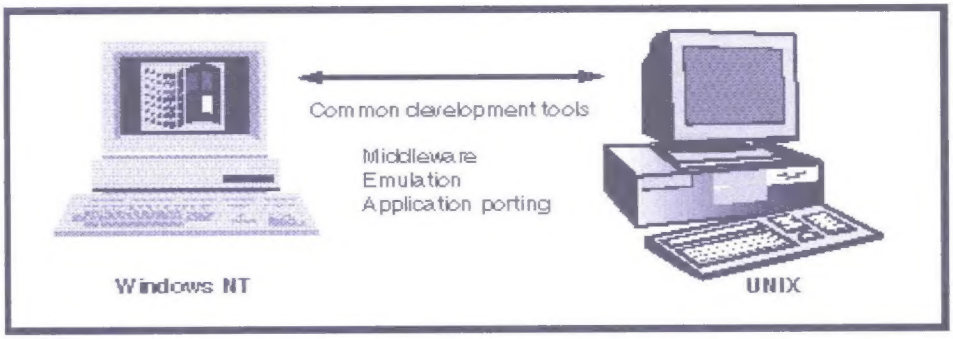
การบริหารจัดการกับระบบรักษาความปลอดภัย

ระบบรักษาความปลอดภัยเครือข่ายเป็นเรื่องที่มีความสำคัญมาก เพราะหัวใจสำคัญของเครือข่ายในประการหนึ่งคือเรื่องของความปลอดภัย ระบบปฏิบัติการแต่ละแบบจะมีเครื่องมือในการจัดตั้งระบบรักษาความปลอดภัยที่แตกต่างกันออกไป ซึ่งต่างมีข้อดีต่างกันด้วย จึงเกิดคำถามว่าท่านควรจะเลือกระบบรักษาความปลอดภัยของใคร เพื่อมิให้เกิดความสับสนและช่วยการบริหารจัดการได้อย่างมีประสิทธิภาพ สามารถแบ่งระบบรักษาความปลอดภัยออกเป็นระดับ (Layer) ต่าง ๆ ได้ดังนี้

- ระบบรักษาความปลอดภัยในเชิงกายภาพ (Physical Security)
- ระบบรักษาความปลอดภัยในระดับของโดเมน (Domain)
- ระบบรักษาความปลอดภัยในระดับของไดเรคทอรี (Directory) และไฟล์ (File)
- ระบบรักษาความปลอดภัยในระดับของผู้ใช้และกลุ่มผู้ใช้ (User & Group)
- ระบบรักษาความปลอดภัยในระดับของเครือข่าย (Network Security)

● ระบบรักษาความปลอดภัยเชิงกายภาพ

ระบบรักษาความปลอดภัยชนิดนี้ครอบคลุมตัวเซิร์ฟเวอร์ต่าง ๆ คอมพิวเตอร์ที่เป็นสถานีทำงานหรือลูกข่ายไปจนถึงอุปกรณ์ของเครือข่าย เช่น Repeater Switches Hub รวมทั้ง Router เป็นต้น การรักษาความปลอดภัยที่ตัวเซิร์ฟเวอร์ ได้แก่ การจำกัดการเข้าถึงอุปกรณ์ต่าง ๆ บนเซิร์ฟเวอร์โดยบุคคลทั่วไป อุปกรณ์ดังกล่าว ได้แก่ ฟลอปปีไดรฟ์ ซีดีรอม คีย์บอร์ด รวมทั้งเมาส์ เป็นต้น ซึ่งสามารถควบคุมได้ด้วยฮาร์ดแวร์หรือซอฟต์แวร์จากผู้ผลิตรายอื่น



รูปที่ 3 แสดงการทำงานร่วมกันระหว่าง Windows NT กับ UNIX

การป้องกันเกี่ยวกับ Repeater Hub ได้แก่ การล็อกตัวฮับให้พ้นมือผู้ไม่หวังดีที่อาจใช้ช่องสื่อสารของฮับที่เหลือเพื่อติดตั้งคอมพิวเตอร์ที่พร้อมด้วยซอฟต์แวร์สำหรับดักจับข้อมูลบนเครือข่าย รวมทั้ง Switches Hub ซึ่งอาจถูกผู้ไม่หวังดีเปลี่ยนแปลงค่า Configuration บางประการที่ท่านติดตั้งไว้เพื่อความปลอดภัย เช่น เปลี่ยนแปลงค่าใน VLAN เป็นต้น นอกจากนี้การปล่อยให้ผู้ประสงค์ร้ายเข้าถึงตัวอุปกรณ์เราเตอร์อาจทำให้เครือข่ายปลายทางที่ท่านกำลังติดต่ออาจเป็นเครือข่ายที่ท่านไม่คาดว่าจะได้รู้จักก็เป็นได้ หากค่า Configuration ของเราเตอร์ถูกเปลี่ยนแปลง

● ระบบรักษาความปลอดภัยในระดับของโดเมน

ระบบปฏิบัติการบางตัว เช่น Windows NT หรือ 2000 จะใช้โดเมนในการบริหารจัดการกับผู้ใช้งานบนเครือข่าย รวมทั้งการจัดการแบ่งปันทรัพยากรให้แก่ผู้ใช้งาน ดังนั้นการวางระบบรักษาความปลอดภัยของโดเมนจึงเป็นเรื่องสำคัญ การวางระบบเครือข่าย Windows NT ในรูปแบบโดเมนสามารถแบ่งออกเป็น 3 รูปแบบดังนี้

1. แบบรวมศูนย์ (Centralized) รูปแบบนี้ทำให้ผู้ใช้ในโดเมนอื่นไม่สามารถเข้ามาดูที่โดเมนหลัก แต่โดเมนหลักเท่านั้นสามารถเข้าไปดูแลจัดการโดเมนอื่น ๆ ได้ วิธีการเช่นนี้ท่านต้องใช้ One-way Trust นอกจากนี้ท่านอาจเลือกให้เครือข่ายมีเพียงโดเมนเดียวก็ได้ โดยผู้ใดที่ประสงค์จะเข้าสู่ระบบเครือข่ายเพื่อใช้ทรัพยากรต้องได้รับการอนุมัติจากผู้ดูแลโดเมนก่อน

2. แบบกระจาย (Decentralized) รูปแบบนี้โดเมนต่าง ๆ บนเครือข่ายจะเป็นอิสระ พร้อมที่จะติดต่อกับโดเมนใด ๆ ก็ได้ โดยมีข้อจำกัดเพียงเล็กน้อยเท่านั้น

3. แบบผสม (Hybrid) เป็นรูปแบบที่รวมเอาแบบที่หนึ่งและสองเข้าด้วยกัน

ผู้ดูแลเครือข่ายจะเลือกรูปแบบใดให้พิจารณาลักษณะการใช้งานแอพพลิเคชัน ข้อจำกัดหรือข้อบังคับต่อผู้ใช้ รวมทั้งลักษณะรูปแบบขององค์กร แผนก รวมทั้งประเภทของข้อมูลอีกด้วย เช่น หากองค์กรของท่านมีหลายแผนก แต่ละแผนกต่างมีข้อมูลลับที่ไม่ต้องการให้แผนกอื่นรับทราบ รวมทั้งการพิมพ์งานไปที่เครื่องพิมพ์จะต้องแยกกัน ท่านควรเลือกใช้แบบรวมศูนย์ ซึ่งอาจต้องแบ่งเป็นหลายโดเมน โดยมีโดเมนหนึ่งเปิดให้ผู้บริหารสามารถเข้าไปเรียกดูข้อมูลของทุกแผนกได้ แต่หากไม่ต้องการให้ผู้ใช้ในโดเมนต่างกันมองเห็นข้อมูล การใช้งานรูปแบบนี้ท่านควรเลือกแบบ Centralized

ระบบปฏิบัติการ NetWare ใช้ซอฟต์แวร์ที่มากับเซิร์ฟเวอร์ชื่อว่า SERMAN.NLM สามารถเรียกจากหน้าจอเซิร์ฟเวอร์ รวมทั้งคำสั่งย่อยหลายตัวเพื่อจัดการกับเซิร์ฟเวอร์

• ระบบรักษาความปลอดภัยในระดับของไดเรคทอรีและไฟล์

ระบบรักษาความปลอดภัยแบบนี้เป็นเรื่องของการกำหนดสิทธิ์ในการเข้าถึงไฟล์และไดเรคทอรีของผู้ใช้งานประเภทรายบุคคลและแบบกลุ่ม ซึ่งเครื่องมือในการรักษาความปลอดภัยได้แก่การกำหนด Permission หรือ Access Rights เป็นสิทธิ์ของการใช้งานหรือเข้าถึงระบบไฟล์หรือไดเรคทอรีแบบใดบ้าง รวมทั้งการกำหนดแอตทริบิวต์ของไฟล์หรือไดเรคทอรี ทั้งนี้เพื่อป้องกันมิให้ทรัพยากรในเครือข่ายเหล่านี้ถูกละเมิดความปลอดภัย ในระบบปฏิบัติการแบบต่าง ๆ จะมีเครื่องมือจัดการเกี่ยวกับระบบไดเรคทอรีหรือไฟล์ให้มาพร้อมอยู่แล้ว เช่น NetWare จะใช้ NDS เพื่อกำหนดความปลอดภัยของไดเรคทอรีและไฟล์ ส่วนระบบปฏิบัติการ UNIX จะใช้คำสั่งซึ่งทำงานบน Command Line หรืออาจใช้เครื่องมือพิเศษที่มากับระบบปฏิบัติการนี้ เช่น Common Desktop Environment (CDE) เพื่อจัดตั้งระบบรักษาความปลอดภัยของไดเรคทอรีและไฟล์ได้เช่นกัน

• ระบบรักษาความปลอดภัยในระดับของผู้ใช้หรือกลุ่มผู้ใช้ (User & Group)

ระบบรักษาความปลอดภัยนี้เริ่มจากการกำหนดให้มีชื่อและรหัสผ่านแก่ผู้ใช้งาน รวมทั้งการกำหนดคุณสมบัติการใช้งานของรหัสผ่าน เป็นต้น ระบบปฏิบัติการโดยทั่วไปมักจะมีระบบรักษาความปลอดภัยที่เกี่ยวกับผู้ใช้งานและกลุ่มของผู้ใช้งาน ซึ่งสามารถแยกออกเป็นหัวข้อได้ดังนี้

- การกำหนดชื่อและรหัสผ่านแก่ผู้ใช้
- การกำหนดคุณสมบัติการทำงานของผู้ใช้และรหัสผ่าน
- การจัดตั้งระบบติดตามการล็อกออนเข้ามาที่เครือข่าย (Logon Auditing)
- การกำหนดสิทธิ์การใช้ไดเรคทอรีและไฟล์ในระดับต่าง ๆ
- การจำกัดสิทธิ์การใช้งานบนเครือข่ายในระดับต่าง ๆ เช่น ข้อจำกัดการใช้เนื้อที่ฮาร์ดดิสก์ หรือใช้เครื่องพิมพ์ เป็นต้น

ในระบบปฏิบัติการ เช่น Windows NT จะมีเครื่องมือที่ใช้บริหารความปลอดภัยแก่ผู้ใช้งานและกลุ่มผู้ใช้งาน ซึ่งได้แก่ User manager for Domain สำหรับ NetWare ท่านสามารถใช้ NDS เพื่อกำหนดบทบาทการทำงานของผู้ใช้งานได้ ส่วนระบบ UNIX ถ้าท่านไม่ใช้คำสั่งการจัดการกับผู้ใช้จาก Command Line จะใช้คำสั่ง Sysadmin ก็ได้

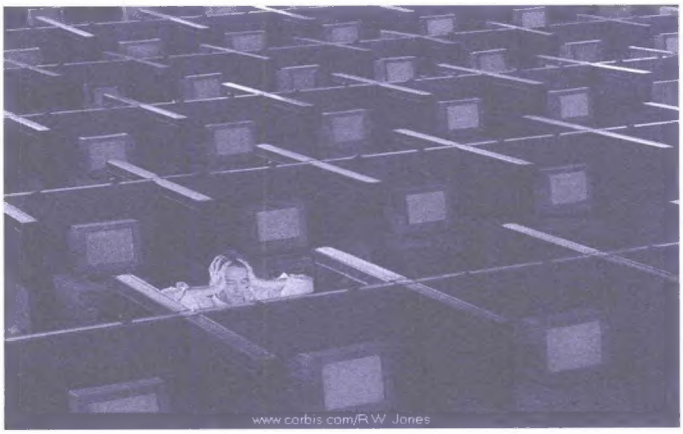
• ระบบรักษาความปลอดภัยในระดับของเครือข่าย

ระบบรักษาความปลอดภัยในระดับนี้เริ่มตั้งแต่การกำหนดเขตแดนในการเข้าสู่เครือข่ายซึ่งกันและกัน เช่น สิทธิ์ในการเข้าไปยังเครือข่ายของอีกฝ่ายหนึ่งที่อาจมาจากระบบปฏิบัติการเดียวกันหรือต่างกันก็ได้ นอกจากนี้ยังครอบคลุมไปถึงการกำหนดมาตรฐานของระบบรักษาความปลอดภัยในการเชื่อมต่อกันระหว่างเครือข่ายที่อยู่ห่างไกล รวมทั้งจัดตั้ง Firewall เพื่อป้องกันภัยอันตรายจากภายนอก หรือจัดตั้งระบบ VPN (Virtual Private Network) สำหรับสื่อสารกันระหว่างผู้ใช้งานที่อยู่ภายนอกองค์กรกับเครือข่ายขององค์กรโดยผ่านทางอินเทอร์เน็ต

สำหรับท่านที่ได้ติดตั้งเว็บเซิร์ฟเวอร์บนระบบ UNIX อาจเลือกใช้ Stronghold3 เป็นเครื่องมือในการป้องกันเว็บเซิร์ฟเวอร์ของท่าน หรือติดตั้ง VPN Server สื่อสารผ่านอินเทอร์เน็ต โดยเลือกใช้โปรโตคอลเพื่อการจัดตั้ง VPN ที่มากับ Windows NT และ Windows 2000 ได้ นอกจากนี้หากท่านเชื่อมต่อกับอินเทอร์เน็ตภายใต้ระบบปฏิบัติการ LINUX ท่านสามารถใช้ Ipchain หรือ Stronghold3 ได้ ในกรณีที่ท่านต้องการกำหนดให้มีระบบการพิสูจน์สิทธิ์เพื่อใช้งานเครือข่ายที่มีประสิทธิภาพสำหรับผู้ที่เข้ามายังเครือข่ายจากระยะไกล ท่านอาจเลือก RADIUS ซึ่งสามารถใช้กับ Windows NT/2000 หรือ UNIX ก็ได้

ในการเลือกใช้เครื่องมือเพื่อจัดตั้งระบบรักษาความปลอดภัย ท่านควรทำเป็นขั้นตอนดังนี้

- กำหนดรูปแบบที่เรียกว่าชั้นหรือ Layer ขึ้นมาเสียก่อน ซึ่งได้กล่าวไว้ในหัวข้อที่แล้ว
- กำหนดมาตรการรักษาความปลอดภัย (Security Policy) ที่สอดคล้องกับลักษณะสภาพแวดล้อมขององค์กรนั้น ๆ ในแต่ละระดับชั้น
- จัดตั้งค่า Configuration ที่เกี่ยวกับระบบรักษาความปลอดภัยในทุกระดับชั้นบนระบบปฏิบัติการทุกตัว โดยใช้เครื่องมือที่มากับระบบปฏิบัติการนั้น ๆ ทำให้เสร็จทีละระบบ
- จัดตั้งระบบรักษาความปลอดภัยในส่วนที่เป็นจุดต่อเชื่อมระหว่างระบบปฏิบัติการ เช่น ผู้ที่จะเข้าไปใช้ทรัพยากรเครือข่ายภายใต้ระบบปฏิบัติการอื่น ๆ จะต้องมีข้อจำกัด รหัสผ่าน และรูปแบบการเข้าถึงเครือข่าย เป็นต้น การจัดตั้งค่าท่านอาจต้องใช้เครื่องมือที่มีอยู่บนระบบปฏิบัติการนั้น ๆ เพื่อให้การสัญจรไปมาระหว่างเครือข่ายต่างระบบปฏิบัติการเป็นแบบไร้รอยตะเข็บ
- ติดตั้งบานประตูหน้าต่างของเครือข่ายให้เรียบร้อย ประตูหน้าคือ Firewall ซึ่งเป็นจุดที่บุคคลภายนอกผ่านเข้ามาที่เครือข่ายของท่าน ส่วนประตูหลังคือทางเข้าออกของเครือข่ายองค์กรที่เชื่อมต่อกับเครือข่ายที่เป็นสาขาขององค์กร ส่วนนี้ท่านอาจจะใช้ซอฟต์แวร์ที่พัฒนาโดยผู้ผลิตรายอื่นเพื่อพิสูจน์สิทธิ์ในการเข้าสู่เครือข่ายขององค์กรหลัก
- หากองค์กรของท่านมีระบบการเข้าถึงเครือข่ายจากบุคคลทั้งภายในและภายนอกองค์กรในรูปแบบของ Remote Access



เพื่อกำหนดคุณสมบัติการทำงานของตัวเครื่องพิมพ์ นอกจากนี้ยังสามารถจัดตั้งระบบรักษาความปลอดภัยในการใช้เครื่องพิมพ์อีกด้วย

นอกจากบริหารจัดการกับเครื่องพิมพ์แล้ว ผู้ดูแลเครือข่ายยังต้องดูแลการใช้งานทรัพยากรอื่น ๆ บนเครือข่าย เช่น ฮาร์ดดิสก์ เป็นต้น

ทั้งในแบบอินทราเน็ตหรืออินเทอร์เน็ต ธรรมดา ท่านควรจัดตั้งระบบ VPN เพื่อป้องกันเครือข่ายอันมีค่าของท่าน

- สุดท้ายคือการจัดตั้งระบบติดตามเฝ้าดู (Auditing & Tracking) รวมทั้งตรวจสอบ (Monitoring) การเข้าออกของผู้ใช้งานตามเซิร์ฟเวอร์ทุกตัว ท่านสามารถจัดตั้งระบบตรวจสอบนี้บนระบบปฏิบัติการหลักทั้ง 3 แบบ ส่วนข้อมูลต่าง ๆ ในรูปของเหตุการณ์ (Event) จะถูกจัดเก็บไว้ใน Log File เพื่อใช้ติดตามเฝ้าดูผู้แปลกปลอมที่อาจเข้ามาที่เครือข่ายได้

การบริหารจัดการกับเครื่องพิมพ์หรือทรัพยากรอื่นบนเครือข่าย

ระบบปฏิบัติการต่าง ๆ จะมีจุดเด่นและจุดด้อยในการควบคุมดูแลการทำงานของเครื่องพิมพ์ที่แตกต่างกัน โดยที่ NetWare มีประสิทธิภาพในการจัดการกับเครื่องพิมพ์มากที่สุด ในขณะที่ Windows NT และ Windows 2000 มีประสิทธิภาพรองลงมา ส่วนระบบ UNIX นั้นรั้งท้ายสุด แต่ไม่ว่าจะใช้ระบบปฏิบัติการใดก็ตาม เครื่องพิมพ์ของท่าน 1 ตัวสามารถถูกแบ่งปันการใช้งานโดยผู้ใช้ที่มาจากระบบปฏิบัติการต่างกันได้

สำหรับ NetWare จะต้องติดตั้งและจัดค่า Configuration ให้กับ Print Server โดยใช้เครื่องมือทางซอฟต์แวร์ที่มาพร้อมกับระบบปฏิบัติการนี้ สำหรับ Windows NT ท่านอาจใช้ Add Printer Wizard จัดตั้งเครื่องพิมพ์ พร้อมกับตั้งค่า Configuration

การบริหารจัดการเพื่อการกู้คืนและสำรองข้อมูล

เรื่องของการทำสำรองข้อมูลเป็นเรื่องที่สำคัญที่สุด เนื่องจากว่าท่านไม่สามารถพยากรณ์ได้ว่า เมื่อใดท่านจะต้องเสียใจเมื่อข้อมูลสูญหาย ส่วนใหญ่ข้อมูลสูญหายล้วนมีสาเหตุมาจากปัญหาไวรัสและปัญหาของอุปกรณ์จัดเก็บข้อมูล เช่น ฮาร์ดดิสก์เสียหายหรือไม่สามารถใช้การได้ เป็นต้น นอกจากนี้ก็เป็นเรื่องรู้เท่าไม่ถึงการณ์ของผู้ใช้งาน ดังนั้นผู้ดูแลเครือข่ายจึงจะต้องกำหนดนโยบายการทำสำรองข้อมูลภายใต้การทำงานของระบบปฏิบัติการที่ต่างกัน ซึ่งแนวทางการกำหนดนโยบายนี้จะต้องเริ่มจากการตั้งคำถามดังต่อไปนี้

- การสำรองข้อมูลนี้จะครอบคลุมไปถึง Server และ Client หรือไม่
- มีคอมพิวเตอร์และไฟล์ใดบ้างสามารถสำรองได้
- จะต้องสำรองข้อมูลบ่อยครั้งเพียงใด
- ใครเป็นผู้สำรองข้อมูล และใครเป็นผู้เก็บบันทึก
- ใครเป็นผู้ที่มีสิทธิ์สำรองข้อมูลแทนผู้ดูแลเครือข่าย
- ใครเป็นผู้ทดสอบและรายงานสถานะของการสำรองข้อมูล
- ลักษณะการจัดเก็บข้อมูลที่สำรองแล้ว
- สถานที่จัดเก็บข้อมูล
- ใครเป็นผู้ Restore ข้อมูลกลับคืนสู่เซิร์ฟเวอร์
- สื่อที่ใช้ในการสำรองข้อมูลมีอะไรบ้าง

ท่านสามารถใช้คำตอบนี้เพื่อสร้างนโยบายการสำรองข้อมูล ระบบปฏิบัติการแต่ละแบบมีเครื่องมือที่ให้ความสะดวกในการจัดทำการสำรองข้อมูลได้เป็นอย่างดี

นอกจากการใช้เครื่องมือเพื่อช่วยสำรองข้อมูลซึ่งมากับระบบปฏิบัติการแล้ว ท่านยังสามารถใช้ซอฟต์แวร์ที่ผลิตโดยผู้ผลิตรายอื่น ๆ ที่มีประสิทธิภาพสูงกว่าเครื่องมือที่มากับระบบปฏิบัติการแน่นอน

การเฝ้าดูและปรับแต่งประสิทธิภาพของเซิร์ฟเวอร์

หน้าที่อีกประการหนึ่งของผู้ดูแลเครือข่ายคือเฝ้าดูและปรับแต่งประสิทธิภาพการทำงานของเซิร์ฟเวอร์ ซึ่งส่งผลต่อประสิทธิภาพการทำงานของเครือข่ายอีกต่อหนึ่ง

ระบบปฏิบัติการหลัก เช่น Windows NT หรือ Windows 2000 Server รวมทั้ง UNIX ต่างมีเครื่องมือที่แฝงมากับระบบปฏิบัติการเหล่านี้ เช่น Windows NT จะใช้ Performance Monitor ช่วยให้ผู้ดูแลเครือข่ายสามารถเฝ้าดูประสิทธิภาพของเซิร์ฟเวอร์ในการทำงาน ซึ่งอาจได้รับผลกระทบมาจากทรัพยากรเชิงฮาร์ดแวร์ของเซิร์ฟเวอร์ เช่น ปริมาณการใช้งานโปรเซสเซอร์ ปริมาณการใช้หน่วยความจำและจำนวนของ Page Fault ที่เกิดขึ้น (การเกิด Page Fault บ่อย ๆ เป็นสัญญาณบ่งชี้ว่าหน่วยความจำบนเซิร์ฟเวอร์ไม่พอส่งผลให้เซิร์ฟเวอร์ทำงานช้าลง) รวมทั้งประสิทธิภาพการทำงานของฮาร์ดดิสก์ในปัจจุบัน นอกจากนี้ยังมีปัจจัยอื่นที่ส่งผลกระทบต่อการทำงานได้ ซึ่ง Performance Monitor จะสามารถชี้ให้เห็นข้อบกพร่องดังกล่าว

ระบบปฏิบัติการ UNIX จะมีคำสั่งหรือโปรแกรมที่เป็นเครื่องมือในการตรวจสอบประสิทธิภาพในการทำงานของเซิร์ฟเวอร์ในรูปแบบ Command Line ตัวอย่างเช่น Perfmeter เพื่อใช้ตรวจสอบดูประสิทธิภาพการทำงานของโปรเซสเซอร์ หน่วยความจำ รวมทั้งดิสก์ และประสิทธิภาพการส่งข้อมูลบนเครือข่าย เป็นต้น

สำหรับ NetWare แม้จะไม่มีคำสั่งที่ใช้เฝ้าดูประสิทธิภาพในการทำงานเซิร์ฟเวอร์โดยตรง แต่ก็สามารถปรับแต่งประสิทธิภาพในการทำงานของเซิร์ฟเวอร์ด้วยคำสั่งประเภท Command Line ซึ่งท่านสามารถใช้บนเซิร์ฟเวอร์ได้เช่นเดียวกัน เช่น การปรับแต่งขนาดของแพ็กเก็ตที่ใช้สื่อสารระหว่างเซิร์ฟเวอร์กับเวิร์กสเตชันของ NetWare และยังมีคำสั่งที่ทำงานบนเซิร์ฟเวอร์ ได้แก่ SCHDELAY.NLM คำสั่ง Memory หรือ Memory Map เป็นต้น อย่างไรก็ดียังมีบริษัทผู้ผลิตซอฟต์แวร์ดี ๆ เพื่อการตรวจสอบและปรับแต่งเซิร์ฟเวอร์หลายตัวซึ่งทำงานบนระบบต่าง ๆ ตัวอย่าง เช่น Trendtrak เป็นต้น

การบริหารจัดการแอพพลิเคชันบนเครือข่าย

แอพพลิเคชันต่าง ๆ เช่น อี-เมล์ และกรุ๊ปแวร์ รวมทั้งดาต้าเบสมักประกอบด้วยส่วนของโปรแกรมที่สำคัญ 2 ประการได้แก่ ส่วนที่เป็นซอฟต์แวร์สำหรับเซิร์ฟเวอร์และซอฟต์แวร์สำหรับไคลเอนต์ ส่วนที่เป็นซอฟต์แวร์สำหรับเซิร์ฟเวอร์ต้องติดตั้งบนเซิร์ฟเวอร์ที่ผู้ใช้งานสามารถเข้าถึงได้ ส่วนซอฟต์แวร์สำหรับไคลเอนต์ใช้ติดตั้งบนเวิร์กสเตชัน ข้อพิจารณาในการเลือกซื้อแอพพลิเคชันท่านอาจต้องใช้แนวคิดดังนี้

- เป็นแอพพลิเคชันที่ใช้งานบนเครือข่าย เนื่องจากแอพพลิเคชันที่ไม่สนับสนุนเครือข่ายจะไม่สามารถทำงานบนเครือข่ายหรือไม่อนุญาตให้ผู้ใช้มากกว่าหนึ่งคนใช้งานร่วมกัน
- เป็นแอพพลิเคชันที่ไม่ต้องใช้เวลาในการจัดการมาก : การติดตั้งแอพพลิเคชันบนเซิร์ฟเวอร์อาจดูง่าย อย่างไรก็ดีการดูแลรักษาและการให้บริการแอพพลิเคชันบนเครือข่ายนั้นเป็นเรื่องยาก เนื่องจากปัญหาของการวางข้อมูลผิดที่ หรือเกิดปัญหาการทำงานค้างที่เวิร์กสเตชันที่มีผลต่อการทำงานของแอพพลิเคชันและข้อมูล รวมทั้งความผิดพลาดที่เกิดจากตัวผู้ใช้เอง ซึ่งท่านอาจจะต้องใช้เวลาน้อยเพื่อแก้ไขปัญหาของแอพพลิเคชันได้อย่างรวดเร็ว
- ใช้เวลาในการโหลดและการเข้าถึงเพื่อใช้งานน้อยที่สุด
- ข้อพิจารณาในเรื่องของการจราจรบนเครือข่าย : การติดตั้งแอพพลิเคชันบนเซิร์ฟเวอร์ เพื่อให้สามารถเข้ามาใช้งานผ่านทางเวิร์กสเตชันเป็นการเพิ่มเส้นทางการสัญจรของข้อมูลข่าวสารบนเครือข่าย ถ้าเป็นการเข้ามาใช้งานของผู้ใช้จากระยะไกลแล้ว ยิ่งเป็นการเพิ่มภาระแก่เครือข่ายมากขึ้น ดังนั้นการโหลดตัวแอพพลิเคชันจะต้องไม่เพิ่มภาระแก่เครือข่ายมาก

เท่าที่กล่าวมานี้เป็นเพียงงานเริ่มต้นเกี่ยวกับการบริหารจัดการแอพพลิชันเท่านั้น ซึ่งงานของผู้ดูแลเครือข่ายดูเหมือนไม่มีวันจบวันสิ้น เนื่องจากมีการปรับปรุงประสิทธิภาพการทำงานในระบบปฏิบัติการเครือข่ายอย่างสม่ำเสมอของผู้ผลิต ทำให้ทักษะการใช้งานและการแสวงหาเครื่องมือสำหรับปรับแต่งประสิทธิภาพของระบบปฏิบัติการกลายเป็นเรื่องจำเป็น

ได้แนวทาง

บทความนี้เขียนขึ้นเพื่อให้ผู้ดูแลเครือข่ายได้มีแนวทางในการดูแลเครือข่ายที่ใช้ระบบปฏิบัติการหลากหลายได้อย่างมีประสิทธิภาพ และเนื่องจากเนื้อที่กระดาษจำกัดจึงไม่อาจลงลึกไปในรายละเอียดตามความตั้งใจ แต่อย่างน้อยคงพอจะเป็นแนวทางได้พอสมควร M

MICRO SHORT TIPS

เทคนิคการค้นหาภาพคลิปอาร์ตจากคีย์เวิร์ด

ตามปกติ Word 2000 สามารถค้นหาภาพคลิปอาร์ตอ้างอิงจากคีย์เวิร์ดที่เกี่ยวข้องกับภาพ เพื่อให้คุณสามารถค้นหาภาพได้อย่างรวดเร็ว โดยไม่จำเป็นต้องเปิดและค้นหาภาพในแต่ละหัวข้อให้เสียเวลา เช่น คุณสามารถค้นหาคลิปอาร์ตที่สัมพันธ์กับคำว่า "ball" โดยไม่จำเป็นต้องค้นหาภาพที่เกี่ยวข้องกับลูกบอลในแต่ละหัวข้อ
ในการค้นหาภาพคลิปอาร์ตด้วยคีย์เวิร์ด ให้คุณทำตามขั้นตอนต่อไปนี้

1. บนเมนูบาร์ เลือกคำสั่ง
2. Insert > Picture > Clip Art
3. คลิกหัวข้อ Search For Clips แล้วป้อนคำที่สัมพันธ์กับภาพที่คุณต้อง
4. การค้นหา จากนั้น Word 2000 จะสร้าง
5. รายการของ
6. ภาพที่ตรง
7. กับคีย์เวิร์ดที่คุณป้อนโดยอัตโนมัติ